]HackingTeam[

RCS Connector

Whitepaper

1 Why integrating?

Remote Control System (RCS) can act as an additional source of data for your established monitoring environment.

Integrating RCS within your current monitoring system will make available new data that otherwise would be impossible to obtain.

Skype calls and encrypted files are unaccessible if not by an RCS Agent running on the monitored device. Having them available side by side with information coming from other sources may dramatically increase the overall value of your solution.

Furthermore, by letting your operators work in an environment they already know you can greatly reduce the startup time for your new RCS installation.

You can integrate RCS with a monitoring center, correlation engine or post processing equipment, such as audio enhancement processors.

1.1 The logic behind it

A Connector is a rule that defines the kind of evidence to be exported and where to store it. You can create multiple Connectors to integrate with multiple system or have different export criteria in place.

Connectors are checked in realtime as soon as an evidence enters the system, thus *minimizing the delay* introduced before the third party system is able to see the new piece of evidence.

Each Connector can be set to export all the incoming evidence, or restricted to a specific Operation, Target or Agent.

1.2 Easy integration with standard formats

Each piece of evidence is exported as a JSON[1] file.

JSON is a widely adopted data-interchange standard, with parsing libraries easily available for almost every programming language.

A raw binary file may accompany the JSON in case of multimedia evidence, such as Skype calls or screenshots.

1.3 Export where you want

Evidence export is done by writing to common Windows folders, thus making exporting to shared network drives, NAS and DAS storage arrays very easy.

Other storage and transport protocols will be supported in the near future.

---

[1] http://www.json.org